ASDI Minimal Audit
Federal Aviation Administration
Traffic Flow Management Program Office
Version 1.2   March 17, 2008

This document consists of the Aircraft Situation Display to Industry (ASDI) Minimal Audit. ASDI Class One display-only data recipients must complete the ASDI Minimal Audit, as described in the "Overview of the ASDI Audit Process" (see reference 2). The audit is a self-audit to be completed by the Class One display-only data recipient.   If they find they are not in compliance with one or more of the audit requirements they should achieve compliance before completing the audit.

Requirements

The requirements that must be satisfied are given below. The requirements are in boldface, explanation of the requirements is in normal type.

1. **The subscriber is eligible to receive the level of data they are being given.** There should be documentation proving the subscriber qualifies for Class One data as defined in the MOA, Section 5.2. Additionally, if the subscriber receives London data, documentation should be provided proving the eligibility for London data as detailed in the MOA, Section 10.

2. **Firewalls are deployed to protect the systems used to view Class One display-only data.** The firewalls may be host-based and run on the hosts used to view Class One data, or they may by used to protect all entrance points to the network, or both network and host-based firewalls may be used.

3. **Firewall policies are restrictive**. Firewall policies are deny-all with exceptions. Exceptions are limited to required functions.

4. **Firewall software is kept up-to-date**. Firewall software is either configured with functional automatic updates or a procedure is in place to obtain security updates as they become available.

5. **If wireless networking is used, then security related vendor defaults are changed from the vendor-supplied defaults. Additional security is in use to protect the network from unauthorized wireless access.** Security related defaults include the default SSID, WPA passphrases, SNMP community strings, and passwords. Additional security should be used, such as firewalls and/or firewall software on wireless routers.

6. **Anti-virus/anti-malware software is deployed on systems used to view Class One display-only data**. This is primarily a Windows requirement. For some operating systems anti-virus/anti-malware software may not be available or useful.

7. **Anti-virus/anti-Malware signatures and software is kept up-to-date.** Security signatures for anti-virus/anti-malware software are updated as they become available.

Signature updates are normally automatic. Software is either configured with functional automatic updates or a procedure is in place to obtain and deploy security updates as they become available.

8. **Access to Class One display-only data is limited to those authorized to access it.** For example, Class One data should not be displayed in the building lobby. For example, network access to Class One data should not be granted to other organizations.

9. **Software, including the operating system, for example Windows or Linux, used on systems accessing display-only data is kept up-to-date with security patches.** Software is either configured with functional automatic updates or a procedure is in place to obtain security updates as they become available. Some organizations may have a procedure in place to test patches before deployment, rather than automatically updating systems.

10. **A strong password policy is used.** Passwords are changed from the vendor-supplied defaults.   Passwords are changed regularly. Passwords used are strong and difficult to crack. Passwordless accounts are not used.

11. **We are familiar with and follow the ASDI MOA.**   All recipients of Class One data must be familiar with the requirements on Class One data as outlined in the "Memorandum of Agreement for Industry Access to the Aircraft Situation Display and National System Status Information Data" (see reference 1).

References

1. "Memorandum of Agreement for Industry Access to the Aircraft Situation Display and National System Status Information Data," Federal Aviation Administration, June 1, 2006. This document, which must be signed by the ASDI direct subscriber, spells out the responsibilities of both the FAA and the direct subscriber. If the direct subscriber violates this MOA, then the direct subscriber is liable to lose access to the feed.

2. "Overview of the ASDI Audit Process," Version 1.2, March 13, 2008. This document includes a description of the three levels of ASDI audit, and how to determine the required level of audit.

For the latest versions of these and other ASDI documents, go to
http://www.fly.faa.gov/ASDI/asdi.html.

Contacts:

For more information about the ASDI Program, contact the ASDI Program Office at
asdi-program-office@faa.gov.

ASDI Minimal Audit Checklist

By December 31 of each year, complete the self-audit and fill in the form below.
Send the notarized copy to your direct/indirect subscriber.

Item	Requirement	Comments	Comply Y/N
1.	The subscriber is eligible to receive the level of data they are being given.		
2.	Firewalls are deployed to protect the systems used to view Class One display-only data.		
3.	Firewall policies are restrictive and based on deny-all with exceptions.		
4.	Firewall software is kept up-to-date.		
5.	If wireless networking is used, then security related vendor defaults are changed from the vendor-supplied defaults and additional security is in use.		
6.	Anti-virus/anti-malware software is deployed on systems used to view Class One display-only data.		
7.	Anti-virus/anti-Malware signatures and software is kept up-to-date.		
8.	Access to display-only data is limited to those authorized to access it.		
9.	Software, including the operating system, for example Windows or Linux, used on systems accessing display-only data is kept up-to-date with security patches.		
10.	A strong password policy is used. Passwords are changed from the vendor-supplied defaults. Passwords are changed regularly. Passwords used are strong and difficult to crack. Passwordless accounts are not used.		
11.	We are familiar with and follow the ASDI MOA.		

Datafeed is received from: _____

Your company name/address: _____

_____

_____

Your name & title _____

Your email address _____

Your telephone number _____

Signature: _____ Date: _____